

“ADS” BODY RECORDER
DATA HANDLING / PROTECTION

10/17/2017

The entire family of Adaptive Digital Systems (ADS), Inc. recorders, namely the EAGLE8, MICRO-FLEX, HAWK, FINCH, FALCON, RAVEN, RAVEN16/32/64/128/256, RAVEN2/2A, DUAL-RAVEN, NANO-RAVEN, NANO-FLEX, NANO-EAGLE, RAVEN-EYE/2/2L/3, RAVEN-GLASS incorporate a multi-layer protection system to ensure the integrity of the evidence collected by the recorder. This system includes data integrity protection during the recording and data integrity protection after the data is downloaded.

During recording the ADS data format partitions the video and audio into small data blocks. A cyclic redundancy code (CRC) value is computed for every one kilobyte of data and added into the data during the recording. The data packaging/encoding and generation of unique CRC features prevent any data modification.

Each time an ADS recording device is turned “OFF” and “ON”, an old session is closed and a new session is created. Any attempt to manipulate the recording by turning the device off and on in the middle of a conversation would generate a separate recording session and would be apparent in the metadata generated by the device and on the computer screen when the user downloads the data containing the recordings. As a result the fact that a recording has only one session means that the recording device ran continuously, without interruption, throughout the conversation.

To ensure the data integrity after being transferred into the storage media, such as DVDs or hard drives, a hash value based on the SHA256 algorithm is generated for every 512 MB of data. When using the ADS software to playback evidence, the data is ‘checksummed’ and verified. If an error is detected a “CHECKSUM ERROR” message is displayed on the computer screen and the recording will not play. Any alteration to the data would be detected on this check.

ADS does not release the source code to anyone, including the Federal, State, and local police agencies, and does not publish where the key codes reside in memory. ADS further controls the opportunity to alter the recordings because the recorder may only be accessed using ADS proprietary software. The ADS software limits user actions to 1. changing performance settings, 2. download, 3. playback/viewing/creation of user copies, and 4. erasure of the data on the recorder.

All of ADS recorders built during the past 30 years have had evidence protection. To my knowledge no evidence has ever been suppressed based upon a challenge to the integrity of an ADS recorder. Any questions or concerns can be addressed to the undersigned.



Attila W. Mathe, President 10/17/17